

**ATTACHMENT B**  
**ITEMS TO BE SEIZED AND SEARCHED**

**Section I**

1. This warrant authorizes the search and seizure of the following items found on the SUBJECT DEVICES listed in Attachment A:

- a. Evidence of who used, owned, or controlled the SUBJECT DEVICES, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Any input/output peripheral devices, passwords, data security devices, and related security documentation that could be related to the SUBJECT DEVICES;
- c. Evidence of software that would allow someone or something other than the user to control the SUBJECT DEVICES, such as viruses, Trojan horses, spyware, malware, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- d. Evidence of the lack of such malicious software on the SUBJECT DEVICES;
- e. Evidence of software designed to protect the SUBJECT DEVICES from other persons, software, devices, or intrusions that may attempt to infiltrate, access, or control the SUBJECT DEVICES, such as pop-up blockers, security software, password protection, and encryption;
- f. Evidence of other storage devices being attached to the SUBJECT DEVICES;
- g. Evidence of counter-forensic programs and hard drive/computer cleaning programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES or frustrate the efforts of law enforcement to locate evidence on the SUBJECT DEVICES;
- h. Evidence of the times the SUBJECT DEVICES was used;
- i. Evidence of where the SUBJECT DEVICES was used, including evidence of wireless Internet networks and Internet Protocol (IP) addresses;
- j. Passwords, encryption keys, and other access devices or programs that may be necessary to access the SUBJECT DEVICES;
- k. Correspondence and contact information pertaining to child pornography or a sexual interest in children;
- l. Documentation and manuals that may be necessary to access the SUBJECT DEVICES or to conduct a forensic examination of the SUBJECT DEVICES;

- m. Records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;
- n. Records of or information about the SUBJECT DEVICES' Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- o. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of SUBJECT DEVICES found; and
- p. Documents and records regarding the ownership and/or possession of the searched premises or SUBJECT DEVICES;
- q. Any child pornography as defined by 18 U.S.C. § 2256(8);
- r. Any material that is "child erotica," consisting of any material or items relating to minors that serves a sexual purpose, including fantasy writings, letters, diaries, books, drawings, and images or videos of minors that do not necessarily constitute child pornography under 18 U.S.C. § 2256(8);
- s. Information or correspondence pertaining to affiliation with any child exploitation websites;
- t. Contextual information necessary to understand the evidence described in this attachment; and
- u. Credit card information, bills, mail, correspondence, and payment records indicating who owns, controls, or resides at the SUBJECT PREMISES and during what time periods.